The overall classification of this presentation is

TOP SECRET//COMINT//NOFORN

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20301108

Welcome to OVSC1204 Business Records (BR) FISA

In this presentation you will receive information from the Office of General Council (OGC) that concerns the metadata obtained pursuant to the Foreign Intelligence Surveillance Act (FISA) Business Records (BR).

At the conclusion of this course there will be a test for BR database access.

Legal Precautions

Examples cited are for training purposes only

The specific details of each operational situation will need to be assessed to ensure correct legal guidance can be provided

Contact Oversight and Compliance (SV) or the Office of General Council (OGC) for assistance

The Office of General Counsel

Roles and Responsibilities of a BR Analyst

A BR-cleared analyst must be able to:

- Describe the framework for BR production and analysis
- Recognize which Foreign Powers are the only authorized targets of this data
- Define the RAS standard
- State the limitations for querying BR data
- Apply correct minimization procedures
- Name points of contact for questions

BRF Metadata

- **Pursuant to Court authorization, NSA is provided telephony metadata**
- NSA is provided the data from [redacted] US service providers?
- Use of data is for protection of the Homeland
- NSA is authorized to conduct contact chaining and [redacted] on the data

Verification Requirement

- Verify that the data is of the type authorized by the order, specifically, call detail records (telephony metadata)
- Under **NO** circumstances may the substantive content of communications be received under this order

Specific Court-Ordered Procedures and Restrictions

The remainder of the slides in this presentation pertain to specific court ordered procedures and restrictions for this authority

Standard for Accessing Data

Any query of the data archive can occur only after a particular known telephone identifier has been associated with either:

- [redacted]
- [redacted]

AND

- The query is based on a Reasonable Articulable Suspicion (RAS)

Standard for Accessing Data

Seed queries must be:

- Specifically known telephone identifiers that meet the targeting standard articulated by the FISA Court (FISC)
    - Examples of Identifiers
        - [redacted]
        - [redacted]
        - Telephone numbers
        - [redacted]
        - As well as other unique identifiers

Standard for Accessing Data

There must be facts giving rise to a *reasonable, articulable suspicion* (RAS) that the original telephone identifier is associated with [redacted]

RAS: Formula

Analysts are NOT free to use a telephone selector based on a hunch or guess.

RAS requires a decision based on **specific facts** that would cause a reasonable person to form such an opinion.

The standard requires some minimal level of objective justification.

First Amendment Considerations

A telephone selector believed to be used by a US person shall not be regarded as associated with [redacted] solely on the basis of activities protected by the First Amendment.

Other Access Requirements

An automatic audit log must be generated for each occasion when the information is accessed.

The Log must contain:

- User Login
- User IP address
- Date and time
- Retrieval request

Manner of Accessing Data

NSA is permitted to perform two types of queries:

1. Contact chaining
2. [redacted]

Minimization Rules

USSID 18 minimization procedures must be applied to the activity

Prior to disseminating any US person identifying information, the Chief of Information Sharing Services must determine that it is related to counterterrorism and that it is necessary to understand or assess the data

Questions?

Office of General Counsel

(Operations/Intel Law)

[redacted]

DL_GCOPS

[redacted]

NSOC has an attorney on call 24/7!

End of BR FISA Video